IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

RYAN MILLIRON, *Plaintiff*, v. UNITED STATES DEPARTMENT OF DEFENSE, *Defendant*.	Civil Action No. 1:23-cv-1222 Hon. Robert J. Jonker U.S. District Judge Hon. Phillip J. Green U.S. Magistrate Judge

EXHIBIT 1
Declaration of Joseph Whited

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF MICHIGAN

RYAN MILLIRON, *Plaintiff*, v. U.S. DEPARTMENT OF DEFENSE, *Defendant*.	Case. No. 23-cv-1222

DECLARATION OF JOSEPH WHITED

Pursuant to 28 U.S.C. § 1746, I, Joseph Whited, hereby declare under penalty of perjury that the following is true and correct:

1. I am the Chief of Staff at the Defense Advanced Research Projects Agency (DARPA) where I support the DARPA Director in managing the Agency's technology portfolio. I have served in this capacity since June 2021. I am also the Acting Director of the Mission Services Office (MSO). In this capacity, I: administer DARPA's Business Process Council (BPC); serve as DARPA's Senior Component Official for Privacy and Civil Liberties; serve as DARPA's Chief Data Officer; oversee the execution of the Freedom of Information Act ("FOIA") function within DARPA; and serve as the Agency's Initial Approval/Denial Authority. I have been a Defense Department Professional for over 10 years and have served in various positions within the Department of Defense, U.S. Navy, and DARPA.

2. The statements in this declaration are based upon my personal knowledge and upon my review of information available to me in my official capacity. Specifically, I am the Acting Director, MSO and DARPA's Initial Approval/Denial Authority. As such, I am familiar

with the September 25, 2023, FOIA request submitted by Plaintiff, Ryan Milliron, seeking "a copy of the August 7, 2016 Fancy Bear/APT 28 Attribution Analysis provided by Manos Antonakakis and David Dagon referenced in the September 25, 2022 letter to Senator [Charles] Grassley." The Department of Defense ("DOD") acknowledged receipt of Plaintiff's FOIA request on September 26, 2023, and assigned it record locator 23-F-1597.

DARPA's Search

3. In response to this FOIA request, DARPA conducted a search of its Information Innovation Office (I2O) using the keywords "APT 28." The Agency located a 40-page report titled "Fancy Bear/APT28 Attribution Analysis," which contains a detailed attribution data analysis of the July 2016 Fancy Bear/APT28 campaign ("the record"). I2O subject matter experts assisted with processing of this record.

Procedural History

4. DARPA's initial review indicated that this record was submitted as part of a technical proposal. As such, Exemption 3, 10 U.S.C. § 3309(b), and Exemption 4 were used to withhold the record in full. Exemptions 3, 50 U.S.C. § 3024(i)(1), 6, 7(E) and 7(F) were also applied to portions of the record. The Office of Secretary of Defense ("OSD") Office of General Counsel ("OGC") notified Plaintiff on March 21, 2024, that the agency was withholding the record in full under Exemptions 3 and 4 (with underlying redactions as indicated).[1]

5. Based on further inquiry by Plaintiff, DARPA re-processed the record and determined that the record was not submitted in conjunction with a formal proposal by Georgia Institute of Technology ("Georgia Tech"). Therefore, DARPA determined that continuing to

[1] The body of the March 21, 2024 email from OSD OGC to Plaintiff states only that the record was withheld in full under Exemption 3 to FOIA. However, each page of the redacted record (which was attached to the March 21, 2024 email) is marked "[Exemption] (b)(4)."

withhold the record in full under Exemption 3, 10 U.S.C. § 3309(b), was not appropriate. In accordance with Executive Order 12,600 ("Predisclosure notification procedures for confidential commercial information") and 32 C.F.R. § 286.10(c), DARPA sent a submitter notice to Georgia Tech on March 28, 2024. Georgia Tech responded to the notice and stated their objection to the release of the record in its entirety under Exemption 4. Based on Georgia Tech's response to the notice, DARPA responded to Plaintiff's request with a denied-in-full response under Exemption 4. Exemptions 3, 50 U.S.C. § 3024(i)(1), 6, and 7(E) were also applied to portions of the record. DARPA's response that it was withholding the record in full under Exemption 4 (with underlying redactions as indicated) was provided to Plaintiff on May 8, 2024.

6. In May 2024, OSD OGC informed DARPA that Plaintiff questioned the use of Exemption 4 to withhold the record in full. Upon further coordination between Georgia Tech and OSD OGC, Georgia Tech agreed to disclose portions of the record, significantly reducing the portions withheld under Exemption 4. At the end of that process of coordination, DOD deemed it appropriate to assert Exemption 4 over significant portions of the information in the record, but not so extensively as Georgia Tech believed appropriate. Ultimately, on November 21, 2024, the Plaintiff was provided 40 pages of responsive records, which were released in part with withholdings made under Exemptions 3, 50 U.S.C. § 3024(i)(1), 4, 6, and 7(E).

Purpose of this Declaration

7. The purpose of this declaration is to explain the basis for DARPA using Exemptions 4, 6, 7(C), and 7(E) to withhold some of the information in the record released to Plaintiff.

Information Redacted Under Exemption 3

8. The version of the report released to Plaintiff contains redactions made pursuant to Exemption 3. DOD has decided not to defend those redactions at summary judgment. Because all of the redactions underlie those made pursuant to other exemptions, including Exemption 4, it is not necessary to release a newly redacted version of the report.

Information Exempt Under Exemption 4

9. Exemption 4, 5 U.S.C. § 552(b)(4), permits the withholding of "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential."

10. Here, DARPA withheld confidential, commercial information obtained from Georgia Tech. DARPA's assertion of Exemption 4 over certain material in the record is based in large part upon Georgia Tech's responses to submitter notices transmitted consistent with Executive Order 12,600 and 34 C.F.R. § 286.10.

11. Georgia Tech submitted the record to DARPA as an unpublished "proof of concept" to illustrate Georgia Tech's capabilities in the area of cyber-attack attribution (for which Georgia Tech later received funding from DARPA). The responsive record at issue, in particular, attributes the July 2016 "hack" of an email server used by the Democratic National Committee. This record was used to illustrate Georgia Tech's unique methodology in attribution, while using a publicly known event so Georgia Tech's conclusions could be verified.

12. Georgia Tech provided this record to DARPA as commercial information illustrating Georgia Tech's capabilities related to forthcoming DARPA research and development (R&D) program efforts, particularly DARPA's Enhanced Attribution program.

Georgia Tech initially responded to DARPA's submitter notice by objecting to the Agency releasing any portion of the record under Exemption 4. As described above, DARPA honored Georgia Tech's request by initially withholding the record in full under Exemption 4.

13. After Plaintiff questioned the propriety of withholding the record in its entirety under Exemption 4, OSD OGC worked with Georgia Tech in an effort to narrow the scope of the university's proposed redactions. OSD OGC and Georgia Tech received multiple rounds of proposed redactions from Georgia Tech. In the end, DOD believed Georgia Tech's proposed redactions to be more extensive than was supportable under the justifications Georgia Tech offered. Accordingly, DOD ultimately adopted the Exemption 4 redactions that appear in the November 2024 release of the record to Plaintiff, which are based on (but more limited than) those redactions that Georgia Tech proposed to DOD.

14. To justify its proposed redactions, Georgia Tech provided to DARPA a draft affidavit describing the reasons for the redactions. That affidavit, which is enclosed as an exhibit to Defendant's motion for summary judgment, is unsigned and in draft form. Although it is unsigned and not final, I understand the affidavit to represent Georgia Tech's final justification for the Exemption 4 withholdings proposed by the university (and a subset of which DOD adopted).

DARPA and the Enhanced Attribution Program

15. DARPA is a research component of DOD.

16. DARPA conducts and funds research programs and projects to enhance the capabilities of the U.S. military.

17. One of DARPA's research programs was called "Enhanced Attribution." As detailed on DARPA's website, that program, (which is now concluded) funded research into

attribution of cyber-attacks (or "hacks") by malicious actors online, which was and is a research priority of the Agency.

Georgia Tech's Information

18. The Georgia Tech affidavit, the reasoning of which DOD has adopted as its own insofar as it supports the Exemption 4 redactions DOD adopted, explains that two categories of information—"statistical features" and "data sources"—must be withheld to avoid potential damage to Georgia Tech's commercial interests. Both of these categories of information are central to the algorithmic attribution technology (described as the "Rhamnousia Framework") whose commercial value is at stake here. I understand the term "statistical features" to refer to aspects of the proprietary algorithm at the heart of Georgia Tech's attribution technology. I understand "data sources" to refer to those sources, public and private, that the algorithm relies on to generate analysis for the laboratory. Together, these features are akin to a combination of a recipe and a roadmap: the recipe combines various sources of data to yield a technology product, which researchers use like a roadmap to find the source of a particular cyber-attack.

19. Astrolavos Lab was and is a research lab at Georgia Tech. Georgia Tech confirmed that Astrolavos Lab submitted the report to DARPA.

20. Confidential statistical features and data sources appear throughout the record:

- In the table of contents (page 2);
- In the abstract (page 2), which gives a high-level overview of the report;
- In the Introduction (pages 2-3), which describes the report's methodology, conclusions, and recommendations;
- In the Analyses (pages 3-18), which contains a sequential description of the steps the researchers took to analyzing and attributing the "hack" at issue. Specifically,

these pages contain a detailed description of the various sources and data on which the researchers brought the algorithm to bear, as well as numerous graphics depicting data sources and workflows;

- In the Recommendations and Additional Comments sections (pages 18-19), which make extensive references to the analyses previously described in the report;
- In the Conclusion (pages 19-20), which briefly describes future research intentions and uses for the algorithm; and
- In the Appendix, which contains detailed descriptions of sources used.

Confidentiality

21. Both the statistical features and the data sources are confidential information. Georgia Tech identified, in Footnote 1 (on page 2 of the record), its intention that the entire record remain confidential for "[U.S. government] internal consideration, not for public distribution." DOD understands that Georgia Tech has customarily kept these statistical features and data sources confidential, as memorialized in the license agreement described in paragraph 24, *infra*. The information was also provided under an implicit assurance from DARPA that it would remain confidential, at least to the extent permitted by law (including FOIA), as the record was provided by Georgia Tech to illustrate the university's capabilities in attribution in anticipation of an upcoming DARPA program (and in contemplation of potential future programs). Such an assurance is customary under the circumstances in which Georgia Tech submitted this record, in particular given the sensitive research that DARPA conducts and funds.

Commercial Nature

22. The methodologies, techniques, and processes described in the proof of concept in the report—including the categories of information that relate to the Rhamnousia Framework, described above—were ultimately made the intellectual property of the Georgia Tech Research Corporation, an affiliate of Georgia Tech.

23. Voreas Laboratories ("Voreas") is a private, for-profit company. Voreas' website describes Voreas as "a DARPA-funded technology spinoff from the Georgia Institute of Technology's Center for Cyber Operations Enquiry and Unconventional Sensing (COEUS)," *see* https://voreas.tech/index.html.

24. Georgia Tech has provided to DOD a copy of an "Exclusive Software License Agreement" concluded in 2019 between the Georgia Tech Research Corporation and Voreas.The agreement memorializes Georgia Tech's ownership, and Voreas' exclusive licensing, of the attribution technology relied upon to produce the record, and desire "to provide for the commercialization" of that technology through a license for its use to Voreas. Georgia Tech independently developed the attribution technology using their unique expertise in internet security, which was then licensed to Voreas. The agreement further requires Voreas to pay consideration to Georgia Tech for its use of the technology. The agreement requires Voreas to keep confidential all "Proprietary Information," a term defined to mean "information and trade secrets owned or controlled by [Georgia Tech Research Corporation] at any time during the term of this Agreement, which relate to the Technology, including but not limited to, invention records, research records and reports, engineering and technical data, designs, production specifications, processes, methods, procedures and facilities."

25. Disclosure of the statistical features and data sources would inhibit the commercial value of Georgia Tech's algorithmic attribution technology, making that information commercial. As described in the Voreas draft affidavit, harm could take two forms. First, an entity with access to the statistical features of the algorithm could "reverse engineer" the algorithm for itself. This would introduce the potential for previously nonexistent competition to Georgia Tech in the attribution space in the form of would-be competitors developing an analogous product and marketing it to interested buyers. Second, commercial harm would result from disclosure in that motivated entities—in particular, the foreign adversaries whose efforts to carry out cyber intrusions (or "hacks") are often exposed by attribution analyses of the sort implicated by the record—would be empowered to take steps to spoil or dilute the data sources on which the algorithm relies, rendering the technology itself useless (and thus unmarketable).

Foreseeable Harm

26. For the same reasons that the confidential information in the report is commercial, *see* ¶¶ 22-25, DARPA foresees that its release would lead to harm of the type Exemption 4 is meant to protect against. In particular, Georgia Tech's commercial, financial interest in its algorithm would be damaged through increased competition, through the elimination of its product's value, or both.

27. Georgia Tech, and its affiliates Astrolavos Lab and Voreas, are established players in the realm of cyber-attack attribution.

28. Malicious actors online have an interest in avoiding detection, and will take steps to do so (including by thwarting technology designed to detect their activities) when possible.

Release of the redacted information would, in turn, make it more possible to avoid detection efforts by Georgia Tech and those entities to which it has licensed its product.

Information Exempt Under Exemption 6 and Exemption 7(C)

29. Exemption 6, 5 U.S.C. § 552(b)(6), permits the Government to withhold personnel, medical, and similar information about individuals when the disclosure of such information "would constitute a clearly unwarranted invasion of personal privacy." DARPA has a longstanding practice of withholding personally identifying information of non-governmental, private persons, as well as its non-public-facing personnel with the military rank of O-6 or below and/or at the civilian pay scale of General Schedule 15 (e.g., GS-15) or below. Exemption 7(C) offers similar protection to personal information that is compiled for law enforcement purposes. Under the practice identified above, DOD protects the same information under Exemption 7(C) where appropriate.

30. The rationale for this policy is that disclosing such information about these individuals, particularly in national security-related matters, could subject them to annoyance, threats, or harassment in their private lives. Moreover, releasing information concerning these non-governmental individuals would not likely serve the "core purpose" of the FOIA, as it would not show "what the government is up to." Thus, any cognizable public interest in releasing this information would not outweigh the significant interest in protecting their personal privacy.

31. Before an agency can invoke any of the harms enumerated in Exemption 7, 5 U.S.C. § 552(b)(7), it must first demonstrate that the records or information at issue were "compiled for law enforcement purposes" (the law enforcement threshold). As noted in the Department of Justice Guide to the Freedom of Information Act for Exemption 7, courts have

recognized that "law enforcement," within the meaning of Exemption 7 can extend beyond traditional law enforcement activities and includes national security and homeland security-related government activities. (Available at https://www.justice.gov/oip/foia-guide/exemption_7/dl). Since its inception, DARPA's mission has been to create technological surprise for U.S. national security. As such, DARPA's work exists to create state-of-the-art technologies that will establish the United States as the leading driver of strategic technological invention. Attribution in general, and the Enhanced Attribution program specifically, seek to identify malicious actors in cyberspace. The stated aim of the program was to "make currently opaque malicious cyber adversary actions and individual cyber operator attribution transparent by providing high-fidelity visibility into all aspects of malicious cyber operator actions and to increase the government's ability to publicly reveal the actions of individual malicious cyber operators without damaging sources and methods." The ability to identify bad actors in cyberspace directly supports DARPA's mission to create technological surprise for national security purposes.

32. Throughout the documents released in this case, DARPA withheld Internet Protocol (IP) addresses, email addresses, names, and photos. IP addresses can be used to reveal a person's general location, Internet Service Provider (ISP), and device. Coupled with other details, information often available from the ISP and/or available to malicious actors, this information can be used to identify an individual. Names, email addresses, and photos can be directly used to identify an individual and, therefore, withheld by DARPA under Exemption 6. Specifically, information protected by Exemption 6 appears in the following locations:

- In three locations on page 6, where non-governmental individuals are mentioned in reference to data sources;

- In one location on page 9, where non-governmental individuals are mentioned in reference to data sources;
- In one location on page 10, where particular domain names and non-governmental entities are mentioned;
- In one location on page 11, where particular domain names and non-governmental entities are mentioned;
- In one location on page 12, where particular domain names and non-governmental entities are mentioned;
- In one location on page 11, where particular domain names and non-governmental entities are mentioned;
- In one location on page 14, where IP addresses, non-governmental email addresses, and URLs are mentioned;
- In two locations on page 16, where particular IP addresses and non-governmental entities are mentioned, and where a photo of two non-governmental individuals appears;
- In one location on page 17, where photos of non-governmental individuals appear; and
- Throughout the Appendix (pages 21-40), where numerous IP addresses, email addresses, and other information pertaining to non-governmental personnel appears.

33. The rationale for this practice is that disclosing this information subjects non-governmental individuals to annoyance, threats, or harassment in their private lives. There is a significant and legitimate personal privacy interest stake and a reasonable probability of future

harassment or a risk of harm or reprisals if this type of information is publicly disclosed. Moreover, releasing these individuals' names and personal information would not serve the "core purpose" of the FOIA, as it would not show "what the government is up to." Thus, there is no public interest outweighing the significant personal privacy interests involved.

34. To my knowledge, none of the individuals whose personally identifiable information appears in the locations listed above have consented to its disclosure.

Information Exempt Under Exemption 7(E)

35. Before an agency can invoke any of the harms enumerated in Exemption 7, 5 U.S.C. § 552(b)(7), it must first demonstrate that the records or information at issue were "compiled for law enforcement purposes" (the law enforcement threshold). For the same reasons given at paragraph 31 above, this threshold is met for the information subject to Exemption 7(E).

36. The "Fancy Bear/APT28 Attribution Analysis" provides a detailed analysis of the July 2016 Fancy Bear/APT28 campaign. Elements of this record, withheld under Exemption 7(E), were used in subsequent DARPA R&D programs with the express intent to assist other agencies with identifying bad cyber actors.

37. Having met the law enforcement threshold, DARPA has specifically asserted Exemption 7(E), 5 U.S.C. § 552(b)(7), which protects information that would otherwise "disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law."

38. The portions of the record withheld under Exemption 7(E) identify specific state-of-the-art techniques to identify bad cyber actors, which is a central part of DARPA's efforts to

protect and detect attacks in the information domain. Among the detailed processes described in the record, the record specifies datasets, location operations, and other sources used to investigate United States adversaries. If released, adversaries would be enabled to circumvent these techniques by modifying their online behaviors to avoid detection. As a result, DARPA's ability to identify malicious activity as part of its national security mission would be hindered (as would, by extension, the ability of other U.S. law enforcement bodies to interdict the behavior of malicious actors online, both criminally and civilly). Additionally, the use of these techniques has expanded beyond the scope of this specific analysis to greater use, both within DARPA R&D programs and other agencies' cyber-related activities.

Review for Reasonably Segregable Information

39. DARPA conducted a line-by-line review of the record for reasonable segregation of non-exempt information and has released that reasonably segregable information where it appears in the record sent to Plaintiff. No further segregation of meaningful information in the redacted record can be made without disclosing information entitled to protection under the FOIA Exemptions invoked above.

I declare under penalty of perjury of the laws of the United States of America that the foregoing is true and correct to the best of my knowledge and information.

Executed this 28th day of February, 2025, in Arlington, Virgina.

Joseph Whited, Chief of Staff